IN THE SPECIFICATION

Please amend the paragraph beginning on page 4, line 25, as follows:

FIG. 1 shows two identity spaces configured to operate as a federation according to the preferred embodiment of the invention. Identity space 105 and identity space ~~110are~~ 110 are typically local computer networks administered by respective owning organization. The computers in the identity space are typically servers such as web servers, proxy servers, directory servers and workstations for end users. Servers such as directory servers typically hold the user identity information in the identity space. The identity information is used by the servers to authenticate the end users whenever they access some resource or service using their work stations.

Please amend the paragraph beginning on page 10, line 11, as follows:

FIG. 2 shows identity spaces 105 and 110 communicating, allowing a user local to identity space 105 to access a resource of identity space 110. Because the user is local to identity space 105 and external to identity space 110, identity space 105 is shown with only forward proxy 205, and identity space 110 is shown with only reverse proxy 210. But a person skilled in the art will recognize that in the preferred embodiment, each identity space in the federation includes both a forward proxy and a reverse proxy. When the user (local to identity space 105) requests access to the resource of identity space 110, forward proxy 205 receives the request (typically from a browser) and routinely forwards access request 212 to identity space 110, as shown by arrow 215. Reverse proxy 210 receives request 212 and consults security module 217 to determine if the resource is restricted or freely available. Security module 217 checks federation access policy 125 to determine whether the resource is protected. If the resource is freely available, reverse proxy 210 allows access to the resource, and the user views the resource as normal.

Please amend the paragraph beginning on page 10, line 24, as follows:

But if the resource is protected, reverse proxy 210 requests that the user authenticate himself. Reverse proxy 210 sends random challenge nonce 218 back to forward proxy 205, as shown by arrow 220. As discussed above, random challenge nonce 218 is used to establish that the user was able to properly authenticate himself to forward proxy 205. Forward proxy 205 requests that the user properly authenticate himself, typically by providing a valid username and password combination. Assuming that the user is able to properly authenticate himself, forward proxy 205 encrypts random challenge nonce 218

provided by reverse proxy 210 using shared long-term secret 120, producing encrypted nonce 222. Forward proxy 205 then returns encrypted nonce 222 to reverse proxy 210, as shown by arrow 225. Forward proxy 205 also ~~places~~ stores temporary data file 227, such as the cookie described above, to remember that the user has been properly authenticated. Reverse proxy 210 independently encrypts random challenge nonce 218. Reverse proxy 210 can then compare encrypted nonce 222 with the result of its (reverse proxy 210) encryption of random challenge nonce 218. If the two match, it establishes that forward proxy 205 properly encrypted random challenge nonce 218, which means that the user was able to properly authenticate himself. Reverse proxy 210 requests that security module 217 check whether the user is authorized to access the resource, using federation access policy 125. If the user is both authenticated and authorized, then reverse proxy 210 permits access to resource 228 by the user from identity space 105, as shown by arrow 230.